Performance and safety construction and evaluation for in-car embedded systems

Françoise Simonot-Lion

Koblenz University

May, 11 2005

aboratoire Lorrain de Recherche en Informatique et ses Applications

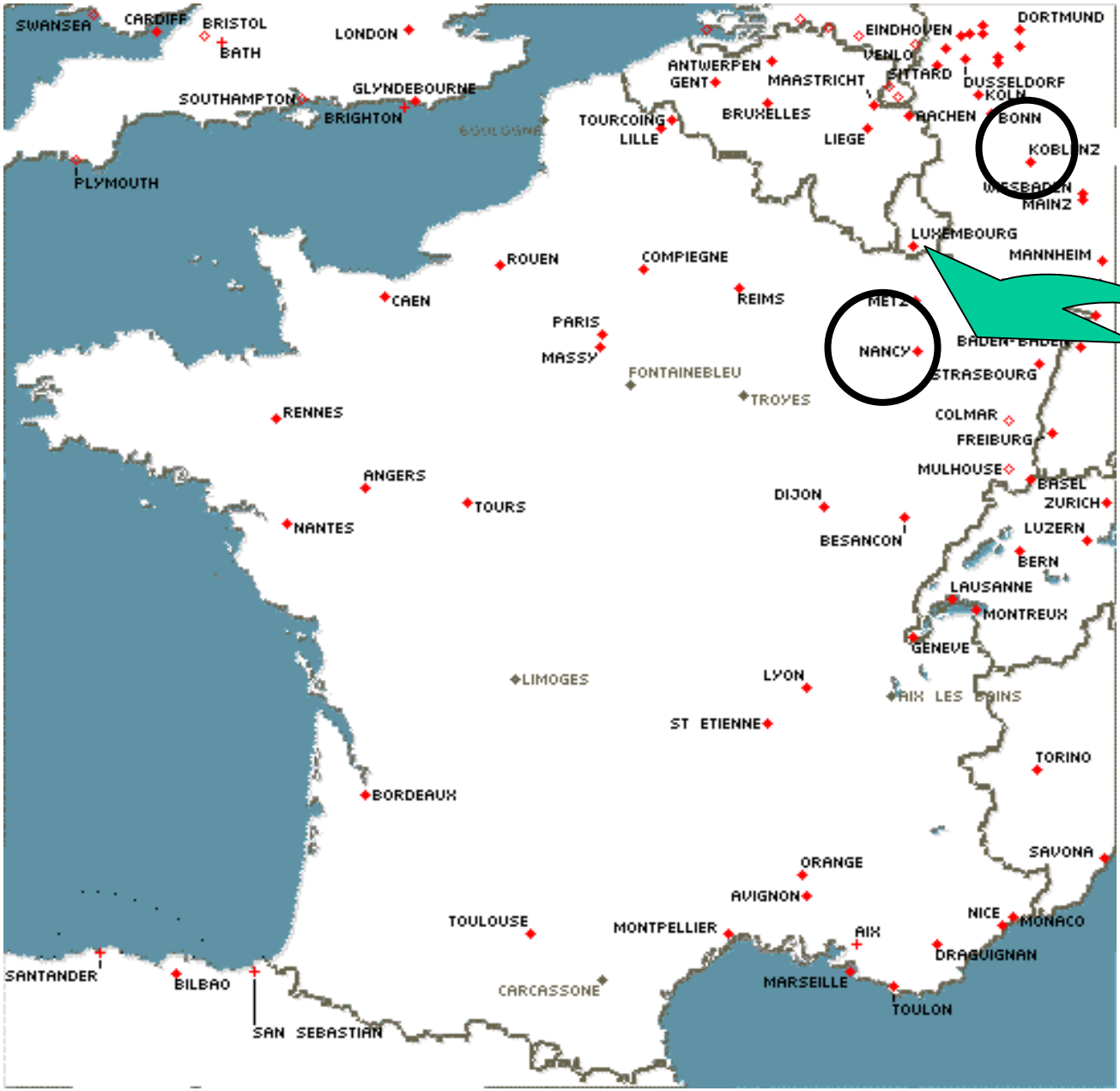
TRIO Team

Performance and safety construction and evaluation for in-car embedded systems

Françoise Simonot – Lion

LORIA (UMR 7503)

simonot@loria.fr



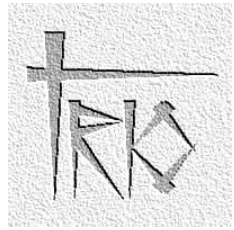
CNRS / INRIA / Universities of Nancy

450 members

UMR 7503

TRIO
Temps Réel et InterOpérabilité
Real Time and InterOperability

INRIA Project Team since january 2002



General objective

To provide techniques and methods for design, validation and scaling real time distributed systems

Keywords:

- **Physical time (Event Driven Timed Systems)**
- **Hardware – Software architectures – OS and protocols – Distribution**
- **Partially known environment - Perturbations**

Research issues

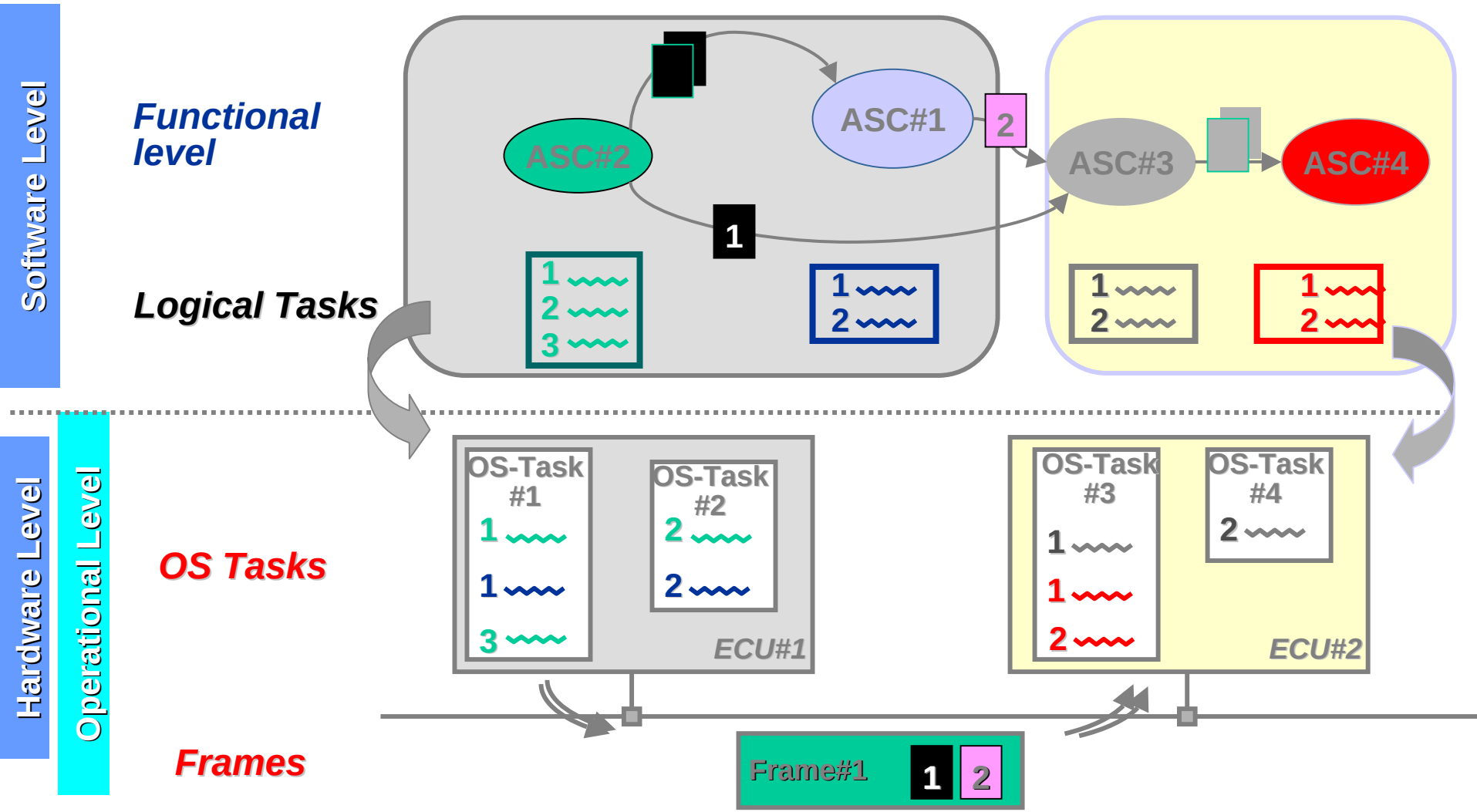
In-Vehicle embedded Systems

- Discrete Event Systems + temporal characteristics → ***Complexity of***
  - ***Modelling***
  - ***Analysis***
- Validation - Scaling → ***Optimisation under constraints (Fault tolerance)***
- Real Time systems
  - Hard real time – Soft real time – Weakly hard real time
- Uncertain environment - perturbations → ***Approaches***
  - ***Deterministic***
  - ***Stochastic***

In-vehicle embedded systems

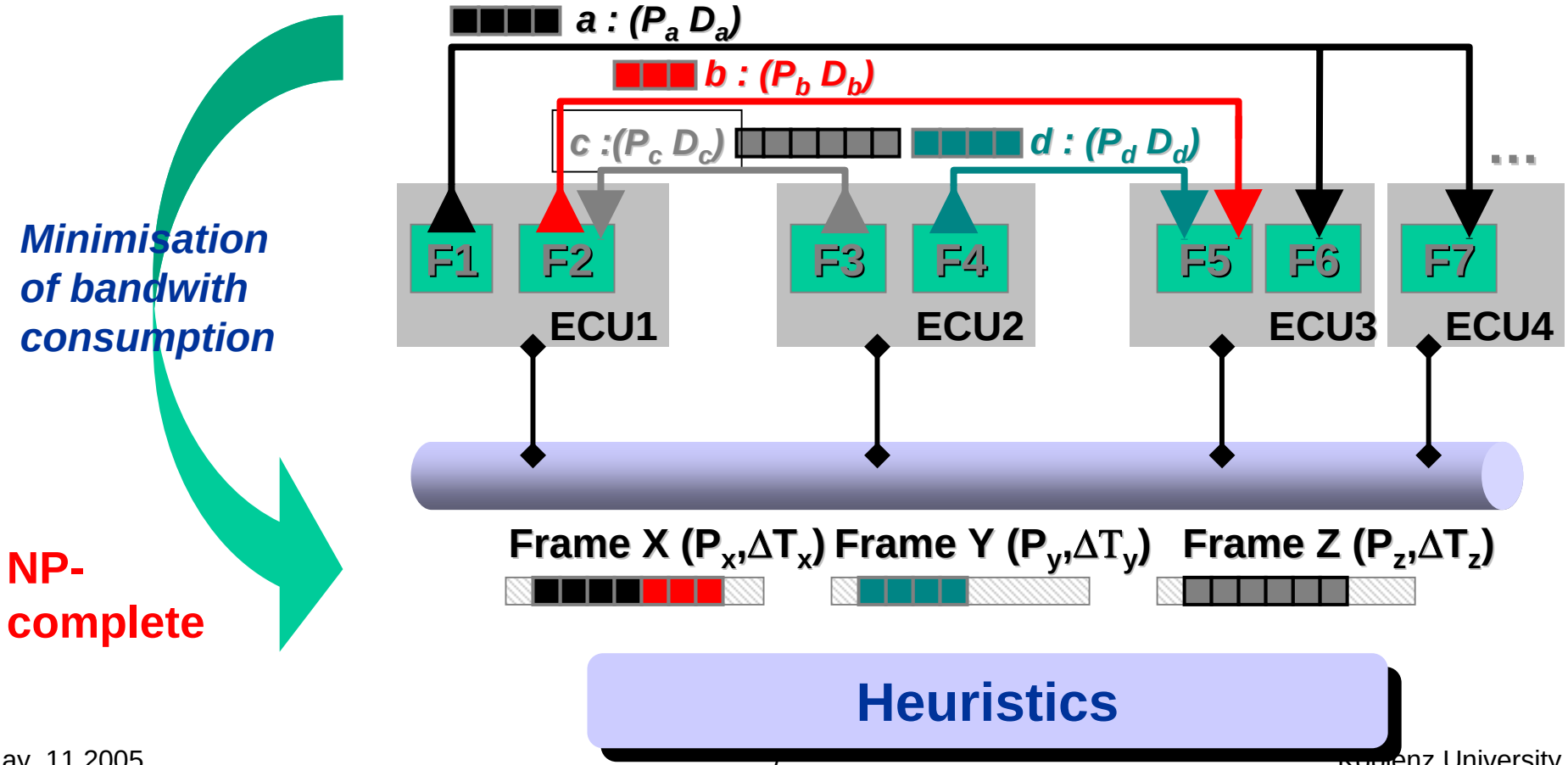
Design and scaling

Modeling the distribution of
logical tasks onto ECU (OS Task)
software flows between distant tasks onto network (Frame)



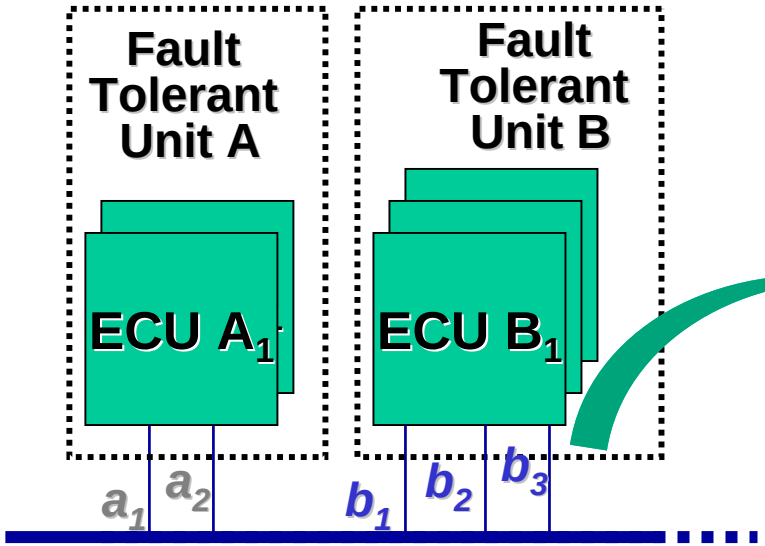
Design and optimal scaling
Priority-based protocol

- **Frame packing under real time constraints :** ***Priority, size, emission rule***



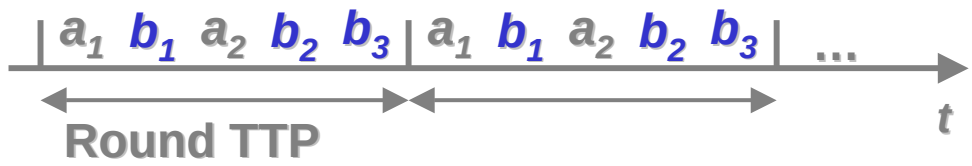
Design and optimal scaling
Time-Triggered protocol

- Redundant nodes – TTP / C protocol – Fault Tolerant Unit



FTU A produces a message a,
period = n_A rounds
FTU B produces a message b
period = n_B rounds

How to allocate the replicated messages in a TTP/C round ?



Error arrival process

Design and optimal scaling
Time-Triggered protocol

- How to place the replicated messages in a TTP/C round ?
  - Fail silent nodes

    To minimize the probability of loss of all the replicated values during a producing period
  - Non Fail silent nodes

    To minimize the probability of loss of at least one replicated values during a producing period

➔Optimal allocation (under assumptions on FTUs)

➔Sub-optimal allocation (heuristics)

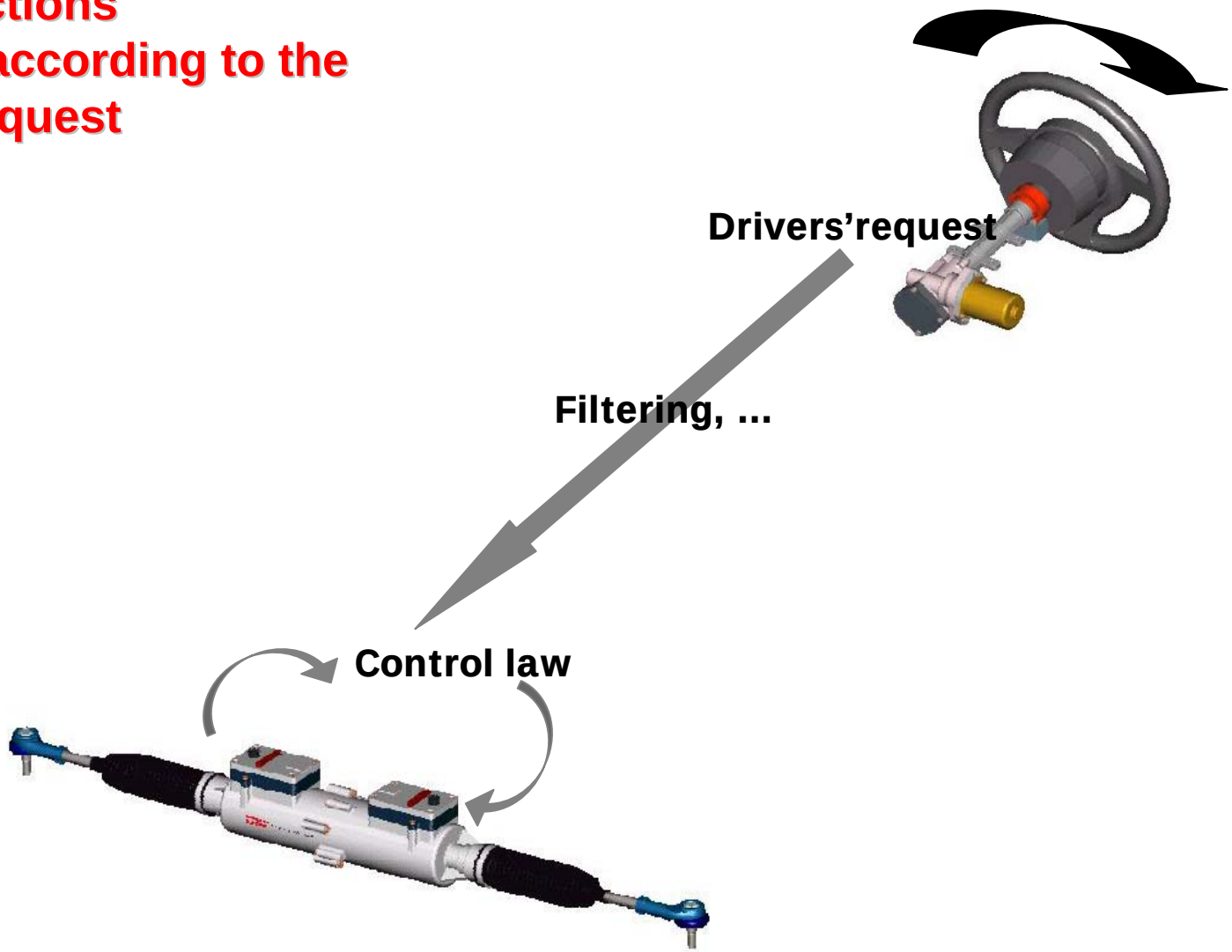
In-vehicle embedded systems

Safety assessment - certification

Steer by Wire systems

Critical functions

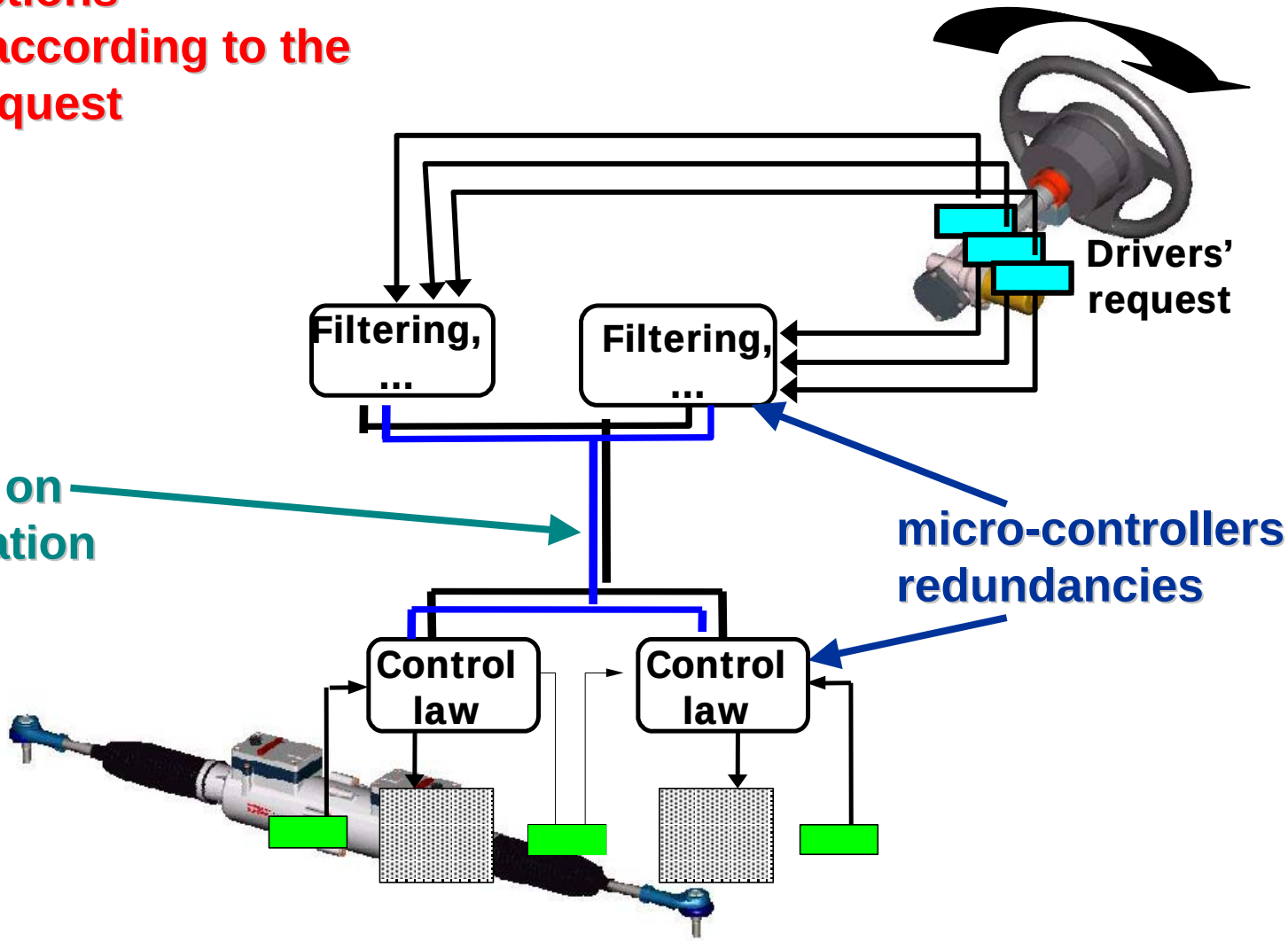
- **Steering according to the drivers' request**



Steer by Wire systems

Critical functions

- **Steering according to the drivers' request**



Steer by Wire systems

Steer-by-Wire is a Safety Critical System

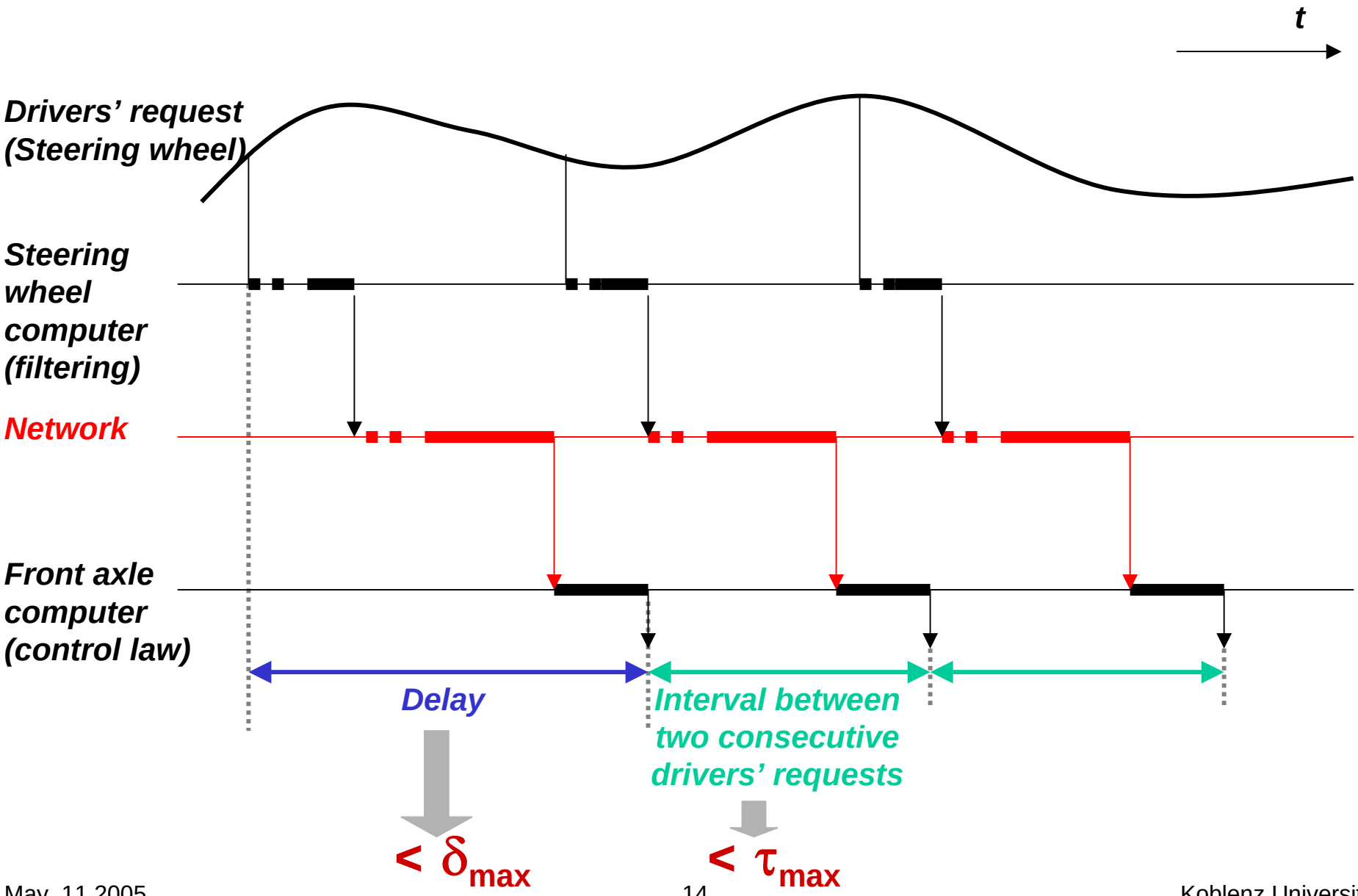
Certification ? Standard ?

CEI 61508 ➔ System Integrity Level (SIL) 4

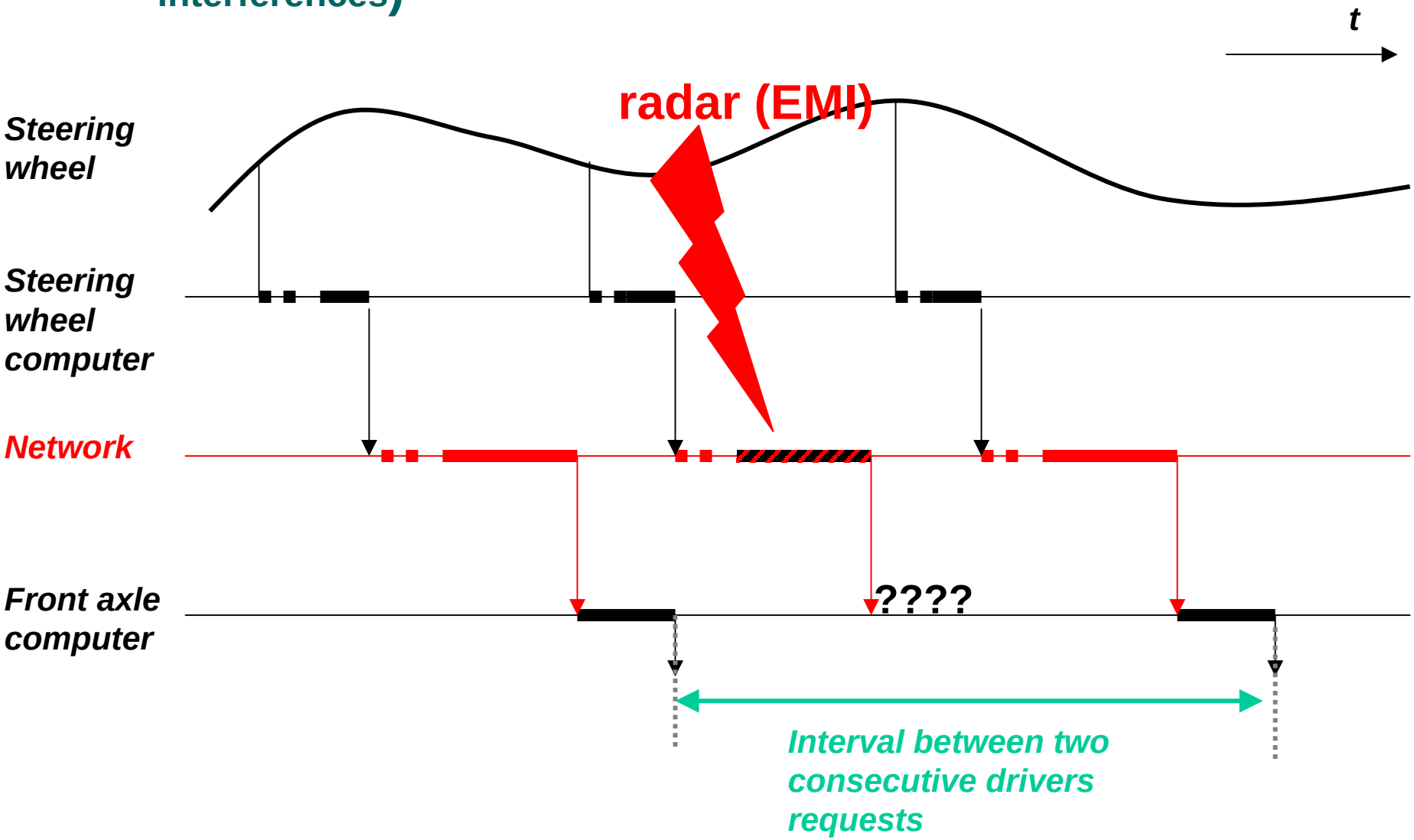
Probability to have a *critical* failure in one hour < 10^{-9}

How to ensure / verify this property
on an
Operational Architecture?

Electronic / software delays - properties



❑ Electronic / software delays under EMI (Electro Magnetic Interferences)



❑ Electronic / software delays under EMI (Electro Magnetic Interferences)

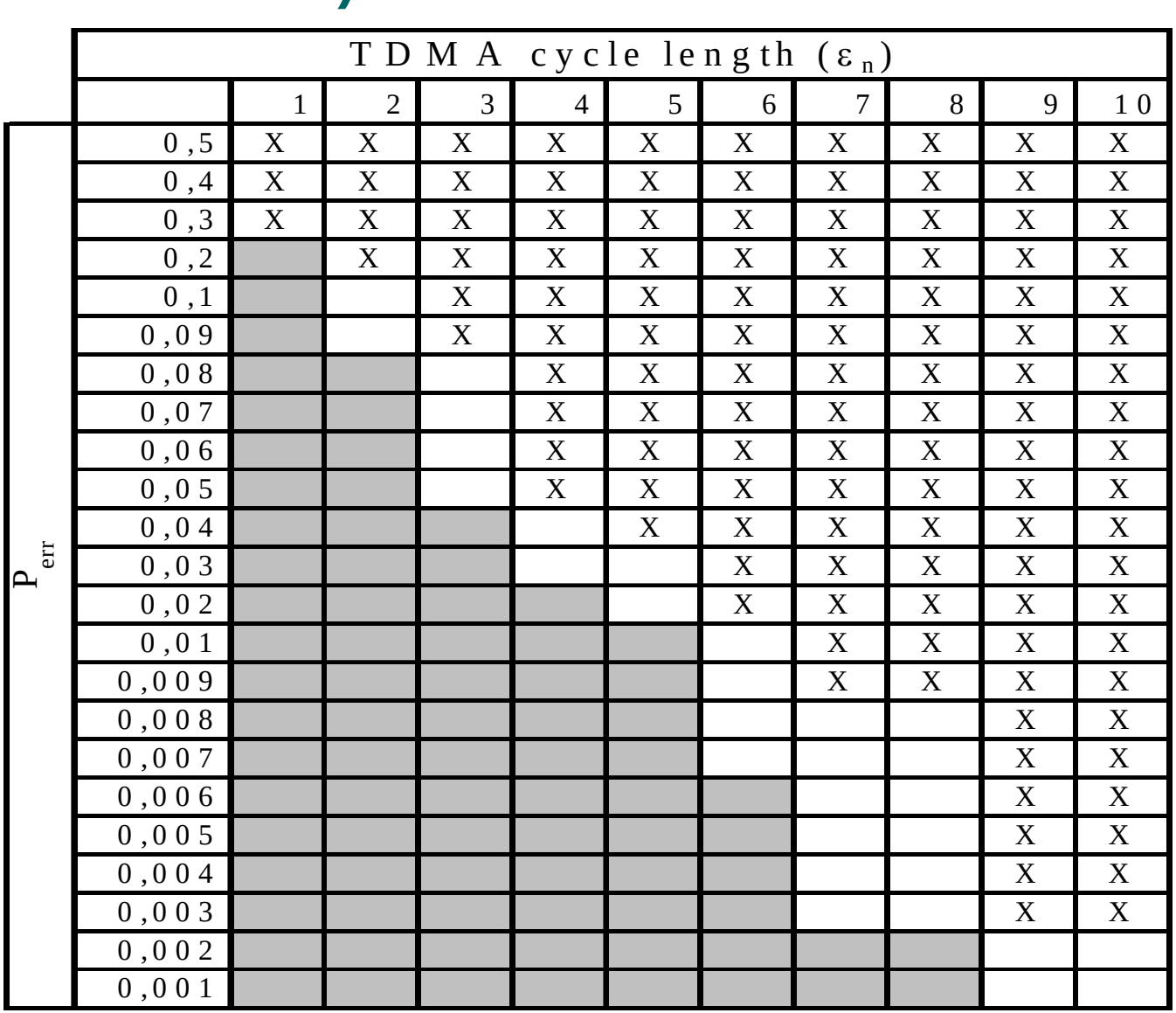
Let us consider:

- **a traject followed by the vehicle (constant vehicle speed),**
- ***Z* a part of this traject subject to EMI**
  - ***L* is the length of *Z* (seconds)**
- **the network is TTP/C**
  - **η_{wc} is the number of TTP rounds in *L***
- **η_{max} is τ_{max}/round size (Matlab / Simulink)**
- **P_{err} is the probability that each round in Z is corrupted**

$$P_{fail}(Z, P_{err}) = 1 - \underbrace{R(\eta_{\max}, \eta_{WC}; P_{err})}$$

Probability to have less than η_{max} consecutive corrupted rounds in η_{wc} rounds

❑ Electronic / software delays under EMI (Electro Magnetic Interferences)



P_{err} \ TDMA cycle length (ε_n)	1	2	3	4	5	6	7	8	9	10
0,5	X	X	X	X	X	X	X	X	X	X
0,4	X	X	X	X	X	X	X	X	X	X
0,3	X	X	X	X	X	X	X	X	X	X
0,2		X	X	X	X	X	X	X	X	X
0,1			X	X	X	X	X	X	X	X
0,09			X	X	X	X	X	X	X	X
0,08				X	X	X	X	X	X	X
0,07				X	X	X	X	X	X	X
0,06				X	X	X	X	X	X	X
0,05				X	X	X	X	X	X	X
0,04					X	X	X	X	X	X
0,03						X	X	X	X	X
0,02						X	X	X	X	X
0,01							X	X	X	X
0,009							X	X	X	X
0,008									X	X
0,007									X	X
0,006									X	X
0,005									X	X
0,004									X	X
0,003									X	X
0,002										
0,001										

X ➔ < 10^{-9}

➔ < 10^{-7} >= 10^{-9}

➔ >= 10^{-7}

For more informations

http://www.loria.fr

http://www.loria.fr/equipes/TRIO/